Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP2005/022788

International filing date: 12 December 2005 (12.12.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-360437
Filing date: 13 December 2004 (13.12.2004)

Date of receipt at the International Bureau: 30 January 2006 (30.01.2006)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 Date of Application:	２００４年１２月１３日
出 願 番 号 Application Number:	特願２００４－３６０４３７
パリ条約による外国への出願に用いる優先権の主張の基礎となる出願の国コードと出願番号 The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is	ＪＰ２００４－３６０４３７
出 願 人 Applicant(s):	松下電器産業株式会社 国立大学法人 東京大学

２００６年 １月１１日

特許庁長官
Commissioner,
Japan Patent Office

中嶋 誠

【書類名】　特許願
【整理番号】　2048160379
【提出日】　平成16年12月13日
【あて先】　特許庁長官　殿
【国際特許分類】　G09C　1/00
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　中野　稔久
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　野仲　真佐男
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　布田　裕一
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　大森　基司
【発明者】
　【住所又は居所】　東京都文京区本郷７－３－１　国立大学法人東京大学内
　【氏名】　五味　剛
【発明者】
　【住所又は居所】　東京都文京区本郷７－３－１　国立大学法人東京大学内
　【氏名】　古原　和邦
【発明者】
　【住所又は居所】　東京都文京区本郷７－３－１　国立大学法人東京大学内
　【氏名】　今井　秀樹
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【特許出願人】
　【識別番号】　504137912
　【氏名又は名称】　国立大学法人東京大学
【代理人】
　【識別番号】　100090446
　【弁理士】
　【氏名又は名称】　中島　司朗
【手数料の表示】
　【予納台帳番号】　014823
　【納付金額】　8,000円
【その他】　国等以外のすべての者の持分の割合１／２
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9003742

【書類名】特許請求の範囲
【請求項１】
コンテンツを利用する利用機器と、利用機器の不正を管理する管理機器と、データを記録する可搬媒体からなる不正機器検知システムであって、
前記利用機器は、当該機器を識別可能な機器識別情報を記憶する記憶部を備え、
前記可搬媒体は、前記機器識別情報を記憶する第1記憶領域、及び当該可搬媒体を識別可能な媒体識別情報を記憶する第2記憶領域を備え、
前記管理機器は、前記可搬媒体の第1記憶領域、及び第2記憶領域からそれぞれ機器識別情報、及び媒体識別情報を読み出す読出部と、前記読み出した機器識別情報、及び媒体識別情報から、前記機器識別情報を保有する利用機器が不正機器か否かを判断する判断部を備えることを特徴とする不正機器検知システム。
【請求項２】
前記不正機器検知システムであって、
前記管理機器は、前記機器識別情報を基準に、媒体識別情報を管理する管理テーブルを生成するテーブル生成部を備えることを特徴とする請求項1記載の不正機器検知システム。
【請求項３】
前記不正機器検知システムであって、
前記管理機器は、不正機器か否かを判断するためのしきい値を記憶するしきい値記憶部を備え、
前記管理機器のテーブル生成部は、機器識別情報を基準に、媒体識別情報をカウントして、前記カウントした総数を記憶する管理テーブルを生成して、
前記管理機器の判断部は、前記カウントした総数が、前記しきい値記憶部に記憶するしきい値を越える場合に不正機器と判断することを特徴とする請求項2記載の不正機器検知システム。
【請求項４】
前記不正機器検知システムであって、
前記管理機器のしきい値記憶部は、機器識別情報ごとに1つ以上のしきい値を記憶することを特徴とする請求項3記載の不正機器検知システム。
【請求項５】
前記著作権保護システムであって、
前記管理機器は、機器識別情報と対応付けてデバイス鍵を記憶するデバイス鍵記憶部と、コンテンツの利用に必要なコンテンツ鍵を選択する選択部と、前記選択部で選択したコンテンツ鍵を、前記機器識別情報に応じたデバイス鍵で暗号化する暗号化部と、前記暗号化したコンテンツ鍵を前記可搬媒体に書き込む書込部を備え、
前記可搬媒体は、前記暗号化コンテンツ鍵を記憶する第3記憶領域を備えることを特徴とする請求項1記載の不正機器検知システム。
【請求項６】
前記不正機器検知システムであって、
前記利用機器は、自身が記憶する機器識別情報が、前記可搬媒体に記憶されているか否かを判断する判断部と、前記判断部で記憶されていないと判断された場合に、前記機器識別情報を前記可搬媒体の前記第1記憶領域に書き込む書込部を備えることを特徴とする請求項1記載の不正機器検知システム。
【請求項７】
前記不正機器検知システムであって、
前記可搬媒体は、コンテンツの利用に必要な暗号化されたコンテンツ鍵を記憶する第3記憶領域を備え、
前記利用機器は、前記可搬媒体が記憶する第3記憶領域から、当該機器に対応する暗号化コンテンツを読み出す読出部を備えることを特徴とする請求項6記載の不正機器検知システム。

【請求項８】
前記不正機器検知システムであって、
前記可搬媒体は、コンテンツの利用に必要な暗号化されたコンテンツ鍵を記憶する第3記憶領域と、前記コンテンツ鍵で暗号化されたコンテンツを記憶する第4記憶領域を備え、
前記利用機器は、前記可搬媒体が記憶する第4記憶領域から、暗号化されたコンテンツを読み出す読出部を備えることを特徴とする請求項7記載の不正機器検知システム。
【請求項９】
前記不正機器検知システムであって、
前記可搬媒体は、コンテンツの利用に必要な暗号化されたコンテンツ鍵を記憶する第3記憶領域を備え、
前記利用機器は、前記可搬媒体が記憶する第3記憶領域から、当該機器が必要な暗号化コンテンツ鍵が存在するか否かを判断する判断部を備えることを特徴とする請求項6記載の不正機器検知システム。
【請求項１０】
前記不正機器検知システムであって、
前記可搬媒体は、メモリーカードであることを特徴とする請求項1記載の不正機器検知システム。
【請求項１１】
前記不正機器検知システムであって、
前記可搬媒体は、ICカードであることを特徴とする請求項1記載の不正機器検知システム。
【請求項１２】
コンテンツを利用する利用機器の不正を管理する管理機器であって、
データを記録する可搬媒体は、前記利用機器を識別可能な機器識別情報を記憶する第1記憶領域、及び当該可搬媒体を識別可能な媒体識別情報を記憶する第2記憶領域を備え、
前記管理機器は、前記可搬媒体の第1記憶領域、及び第2記憶領域からそれぞれ機器識別情報、及び媒体識別情報を読み出す読出部と、前記読み出した機器識別情報、及び媒体識別情報から、前記機器識別情報を保有する利用機器が不正機器か否かを判断する判断部を備えることを特徴とする管理機器。
【請求項１３】
前記管理機器であって、
前記管理機器は、前記機器識別情報を基準に、媒体識別情報を管理する管理テーブルを生成するテーブル生成部を備えることを特徴とする請求項12記載の管理機器。
【請求項１４】
前記管理機器であって、
前記管理機器は、不正機器か否かを判断するためのしきい値を記憶するしきい値記憶部を備え、
前記管理機器の管理テーブル生成部は、機器識別情報を基準に媒体識別情報をカウントして、前記カウントした総数を記憶する管理テーブルを生成して、
前記管理機器の判断部は、前記カウントした総数が、前記しきい値記憶部に記憶するしきい値を越える場合に不正機器と判断することを特徴とする請求項13記載の管理機器。
【請求項１５】
前記管理機器であって、
前記管理機器のしきい値記憶部は、機器識別情報ごとに１つ以上のしきい値を記憶することを特徴とする請求項14記載の管理機器。
【請求項１６】
前記管理機器であって、
前記管理機器は、機器識別情報と対応付けてデバイス鍵を記憶するデバイス鍵記憶部と、コンテンツの利用に必要なコンテンツ鍵を選択する選択部と、前記選択部で選択したコ

ンテンツ鍵を、前記機器識別情報に応じたデバイス鍵で暗号化する暗号化部と、前記暗号化したコンテンツ鍵を前記可搬媒体に書き込む書込部を備えることを特徴とする請求項12記載の管理機器。

【請求項１７】

コンテンツを利用する利用機器であって、

データを記録する可搬媒体は、前記利用機器を識別可能な機器識別情報を記憶する第1記憶領域、及び当該可搬媒体を識別可能な媒体識別情報を記憶する第2記憶領域を備え、

前記利用機器は、当該機器を識別可能な機器識別情報を記憶する記憶部を備えることを特徴とする利用機器。

【請求項１８】

前記利用機器であって、

前記利用機器は、自身が記憶する機器識別情報が、前記可搬媒体に記憶されているか否かを判断する判断部と、前記判断部で記憶されていないと判断された場合に、前記機器識別情報を前記可搬媒体の前記第1記憶領域に書き込む書込部を備えることを特徴とする請求項17記載の利用機器。

【請求項１９】

前記利用機器であって、

前記可搬媒体は、コンテンツの利用に必要な暗号化されたコンテンツ鍵を記憶する第3記憶領域を備え、

前記利用機器は、前記可搬媒体が記憶する第3記憶領域から、当該機器に対応する暗号化コンテンツを読み出す読出部を備えることを特徴とする請求項18記載の利用機器。

【請求項２０】

前記利用機器であって、

前記可搬媒体は、コンテンツの利用に必要な暗号化されたコンテンツ鍵を記憶する第3記憶領域と、前記コンテンツ鍵で暗号化されたコンテンツを記憶する第4記憶領域を備え、

前記利用機器は、前記可搬媒体が記憶する第4記憶領域から、暗号化されたコンテンツを読み出す読出部を備えることを特徴とする請求項21記載の利用機器。

【請求項２１】

前記利用機器であって、

前記可搬媒体は、コンテンツの利用に必要な暗号化されたコンテンツ鍵を記憶する第3記憶領域を備え、

前記利用機器は、前記可搬媒体が記憶する第3記憶領域から、当該機器が求める暗号化コンテンツ鍵が存在するか否かを判断する判断部を備えることを特徴とする請求項18記載の利用機器。

【請求項２２】

データを記録する可搬媒体であって、

前記可搬媒体は、コンテンツを利用する利用機器を識別可能な機器識別情報を記憶する第1記憶領域、及び当該可搬媒体を識別可能な媒体識別情報を記憶する第2記憶領域を備えることを特徴とする可搬媒体。

【請求項２３】

前記可搬媒体であって、

前記可搬媒体は、コンテンツの利用に必要な暗号化されたコンテンツ鍵を記憶する第3記憶領域を備えることを特徴とする請求項22記載の可搬媒体。

【請求項２４】

前記可搬媒体であって、

前記可搬媒体は、メモリーカードであることを特徴とする請求項22記載の可搬媒体。

【請求項２５】

前記可搬媒体であって、

前記可搬媒体は、ICカードであることを特徴とする請求項22記載の可搬媒体。

【請求項２６】
不正利用を管理する管理機器と、データを記録する可搬媒体からなる不正利用検知システムであって、
前記可搬媒体は、利用機器を識別可能な機器識別情報を記憶する第1記憶領域、及び当該可搬媒体を識別可能な媒体識別情報を記憶する第2記憶領域を備え、
前記管理機器は、前記可搬媒体の第1記憶領域、及び第2記憶領域からそれぞれ機器識別情報、及び媒体識別情報を読み出す読出部と、前記読み出した機器識別情報、及び媒体識別情報から、前記機器識別情報を保有する利用機器が不正利用されたか否かを判断する判断部を備えることを特徴とする不正利用検知システム。
【請求項２７】
前記不正利用検知システムであって、
前記管理機器は、前記機器識別情報と前記媒体識別情報の組を管理する管理テーブルを生成するテーブル生成部と、前記媒体識別情報を基準にして、異なる機器識別情報を入手した場合に当該利用を不正と判断する判断部を備えることを特徴とする請求項26記載の不正利用検知システム。
【請求項２８】
前記不正利用検知システムであって、
前記管理機器は、前記媒体固有情報ごとに異なるしきい値を設けて記憶する記憶部を備えることを特徴とする請求項26記載の不正利用検知システム。
【請求項２９】
不正利用を管理する管理機器であって、
データを記録する可搬媒体は、利用機器を識別可能な機器識別情報を記憶する第1記憶領域、及び当該可搬媒体を識別可能な媒体識別情報を記憶する第2記憶領域を備え、
前記管理機器は、前記可搬媒体の第1記憶領域、及び第2記憶領域からそれぞれ機器識別情報、及び媒体識別情報を読み出す読出部と、前記読み出した機器識別情報、及び媒体識別情報から、前記機器識別情報を保有する利用機器が不正利用されたか否かを判断する判断部を備えることを特徴とする管理機器。
【請求項３０】
前記管理機器であって、
前記管理機器は、前記機器識別情報と前記媒体識別情報の組を管理する管理テーブルを生成するテーブル生成部と、前記媒体識別情報を基準にして、異なる機器識別情報を入手した場合に当該利用を不正と判断する判断部を備えることを特徴とする請求項31記載の管理機器。
【請求項３１】
前記管理機器であって、
前記管理機器は、前記媒体固有情報ごとに異なるしきい値を設けて記憶する記憶部を備えることを特徴とする請求項29記載の管理機器。
【請求項３２】
コンテンツを利用する利用機器と、利用機器の不正を管理する管理機器と、データを記録する可搬媒体からなる不正機器検知方法であって、
前記利用機器は、当該機器を識別可能な機器識別情報を記憶する記憶ステップを備え、
前記可搬媒体は、前記機器識別情報を記憶する第1記憶ステップ、及び当該可搬媒体を識別可能な媒体識別情報を記憶する第2記憶ステップを備え、
前記管理機器は、前記可搬媒体の第1記憶領域、及び第2記憶領域からそれぞれ機器識別情報、及び媒体識別情報を読み出す読出ステップと、前記読み出した機器識別情報、及び媒体識別情報から、前記機器識別情報を保有する利用機器が不正機器か否かを判断する判断ステップを備えることを特徴とする不正機器検知方法。

【書類名】明細書
【発明の名称】不正機器検知システム、不正利用検知システム、及び方法
【技術分野】
【０００１】
本発明は、映画や音楽などの著作物であるコンテンツのデジタル化データを再生するシステムに関し、特に不正機器を利用したコンテンツの再生による著作権侵害を防止するために、不正機器を発見、あるいは特定する不正機器検知システムに関する。
【背景技術】
【０００２】
近年、マルチメディア関連技術の発展、大容量記録媒体の出現等を背景として、動画、音声等からからなるデジタルコンテンツ（以下、コンテンツ）を生成して、光ディスク等の大容量記録媒体に格納して配布する、あるいはネットワークや放送を介して配信するシステムが登場している。
一般的に、コンテンツの著作権を保護するため、即ちコンテンツの不正再生や不正コピーといった不正利用を防止するために暗号化技術が用いられる。
【０００３】
具体的には、コンテンツをある暗号化鍵を用いて暗号化して光ディスク等の記録媒体に記録して配布する。これに対して、その暗号化鍵に対応する復号鍵を保有する端末のみが、記録媒体から読み出したデータをその復号鍵を用いて復号して、コンテンツの再生等を行うことができる、というものである。なお、コンテンツを暗号化して記録媒体に記録する方法としては、端末が保有する復号鍵に対応する暗号化鍵でコンテンツそのものを暗号化して記録する方法や、コンテンツをある鍵で暗号化して記録した上で、その鍵に対応する復号用の鍵を、端末が保有する復号鍵に対応する暗号化鍵で暗号化して記録する方法等がある。
【０００４】
このとき、端末が保有する復号鍵は外部に露見しないように厳重に管理される必要があるが、不正者による端末内部の解析において、ある鍵が外部に暴露される危険性がある。ある鍵が一旦不正者に暴露されてしまうと、コンテンツを不正利用する記録装置、再生装置、あるいはソフトウェアを作成して、インターネット等によりそれらを流布することが考えられる。このような場合、著作権者は一旦暴露された鍵では、次から提供するコンテンツを扱えないようにしたいと考える。これを鍵無効化技術と呼び、鍵無効化を実現するシステムとして、特許文献1、あるいは特許文献2が開示されている。
【特許文献１】特開2000-31922号公報
【特許文献２】特開2002-281013号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかしながら、前記鍵無効化技術が開示されている特許文献においては、外部に漏れた鍵（無効化すべき鍵）を特定する方法については開示されておらず、特定するためには、市場に大量流通した不正機器／不正ソフトウェアを回収して、内部を解析することでしか特定できないという課題を有していた。
本発明は、前記課題を解決するもので、可搬媒体の固有IDを利用して、効率的に無効化すべき鍵を発見、あるいは特定することが可能な不正機器検知システムを提供することを目的とする。
【課題を解決するための手段】
【０００６】
本発明は、コンテンツを利用する利用機器と、利用機器の不正を管理する管理機器と、データを記録する可搬媒体からなる不正機器検知システムであって、前記利用機器は、当該機器を識別可能な機器識別情報を記憶する記憶部を備え、前記可搬媒体は、前記機器識別情報を記憶する第1記憶領域、及び当該可搬媒体を識別可能な媒体識別情報を記憶する

第2記憶領域を備え、前記管理機器は、前記可搬媒体の第1記憶領域、及び第2記憶領域からそれぞれ機器識別情報、及び媒体識別情報を読み出す読出部と、前記読み出した機器識別情報、及び媒体識別情報から、前記機器識別情報を保有する利用機器が不正機器か否かを判断する判断部を備えることを特徴とする。

【０００７】

また、本発明は、前記不正機器検知システムであって、前記管理機器は、前記機器識別情報を基準に、媒体識別情報を管理する管理テーブルを生成するテーブル生成部を備えることを特徴とする。

また、本発明は、前記不正機器検知システムであって、　前記管理機器は、不正機器か否かを判断するためのしきい値を記憶するしきい値記憶部を備え、前記管理機器のテーブル生成部は、機器識別情報を基準に、媒体識別情報をカウントして、前記カウントした総数を記憶する管理テーブルを生成して、前記管理機器の判断部は、前記カウントした総数が、前記しきい値記憶部に記憶するしきい値を越える場合に不正機器と判断することを特徴とする。

【０００８】

また、本発明は、前記不正機器検知システムであって、　前記管理機器のしきい値記憶部は、機器識別情報ごとに1つ以上のしきい値を記憶することを特徴とする。

また、本発明は、前記著作権保護システムであって、前記管理機器は、機器識別情報と対応付けてデバイス鍵を記憶するデバイス鍵記憶部と、コンテンツの利用に必要なコンテンツ鍵を選択する選択部と、前記選択部で選択したコンテンツ鍵を、前記機器識別情報に応じたデバイス鍵で暗号化する暗号化部と、前記暗号化したコンテンツ鍵を前記可搬媒体に書き込む書込部を備え、前記可搬媒体は、前記暗号化コンテンツ鍵を記憶する第3記憶領域を備えることを特徴とする。

【０００９】

また、本発明は、前記不正機器検知システムであって、　前記利用機器は、自身が記憶する機器識別情報が、前記可搬媒体に記憶されているか否かを判断する判断部と、前記判断部で記憶されていないと判断された場合に、前記機器識別情報を前記可搬媒体の前記第1記憶領域に書き込む書込部を備えることを特徴とする。

また、本発明は、前記不正機器検知システムであって、前記可搬媒体は、コンテンツの利用に必要な暗号化されたコンテンツ鍵を記憶する第3記憶領域を備え、前記利用機器は、前記可搬媒体が記憶する第3記憶領域から、当該機器に対応する暗号化コンテンツを読み出す読出部を備えることを特徴とする。

【００１０】

また、本発明は、前記不正機器検知システムであって、　前記可搬媒体は、コンテンツの利用に必要な暗号化されたコンテンツ鍵を記憶する第3記憶領域と、前記コンテンツ鍵で暗号化されたコンテンツを記憶する第4記憶領域を備え、前記利用機器は、前記可搬媒体が記憶する第4記憶領域から、暗号化されたコンテンツを読み出す読出部を備えることを特徴とする。

【００１１】

また、本発明は、前記不正機器検知システムであって、　前記可搬媒体は、コンテンツの利用に必要な暗号化されたコンテンツ鍵を記憶する第3記憶領域を備え、前記利用機器は、前記可搬媒体が記憶する第3記憶領域から、当該機器が必要な暗号化コンテンツ鍵が存在するか否かを判断する判断部を備えることを特徴とする。

また、本発明は、前記不正機器検知システムであって、　前記可搬媒体は、メモリーカードであることを特徴とする。

【００１２】

また、本発明は、前記不正機器検知システムであって、前記可搬媒体は、ICカードであることを特徴とする。

また、本発明は、コンテンツを利用する利用機器の不正を管理する管理機器であって、データを記録する可搬媒体は、前記利用機器を識別可能な機器識別情報を記憶する第1記

憶領域、及び当該可搬媒体を識別可能な媒体識別情報を記憶する第2記憶領域を備え、前記管理機器は、前記可搬媒体の第1記憶領域、及び第2記憶領域からそれぞれ機器識別情報、及び媒体識別情報を読み出す読出部と、前記読み出した機器識別情報、及び媒体識別情報から、前記機器識別情報を保有する利用機器が不正機器か否かを判断する判断部を備えることを特徴とする。

【００１３】

また、本発明は、前記管理機器であって、前記管理機器は、前記機器識別情報を基準に、媒体識別情報を管理する管理テーブルを生成するテーブル生成部を備えることを特徴とする。

また、本発明は、前記管理機器であって、　前記管理機器は、不正機器か否かを判断するためのしきい値を記憶するしきい値記憶部を備え、前記管理機器の管理テーブル生成部は、機器識別情報を基準に媒体識別情報をカウントして、前記カウントした総数を記憶する管理テーブルを生成して、前記管理機器の判断部は、前記カウントした総数が、前記しきい値記憶部に記憶するしきい値を越える場合に不正機器と判断することを特徴とする。

【００１４】

また、本発明は、前記管理機器であって、　前記管理機器のしきい値記憶部は、機器識別情報ごとに１つ以上のしきい値を記憶することを特徴とする。

また、本発明は、前記管理機器であって、前記管理機器は、機器識別情報と対応付けてデバイス鍵を記憶するデバイス鍵記憶部と、コンテンツの利用に必要なコンテンツ鍵を選択する選択部と、前記選択部で選択したコンテンツ鍵を、前記機器識別情報に応じたデバイス鍵で暗号化する暗号化部と、前記暗号化したコンテンツ鍵を前記可搬媒体に書き込む書込部を備えることを特徴とする。

【００１５】

また、本発明は、コンテンツを利用する利用機器であって、データを記録する可搬媒体は、前記利用機器を識別可能な機器識別情報を記憶する第1記憶領域、及び当該可搬媒体を識別可能な媒体識別情報を記憶する第2記憶領域を備え、前記利用機器は、当該機器を識別可能な機器識別情報を記憶する記憶部を備えることを特徴とする。

また、本発明は、前記利用機器であって、前記利用機器は、自身が記憶する機器識別情報が、前記可搬媒体に記憶されているか否かを判断する判断部と、前記判断部で記憶されていないと判断された場合に、前記機器識別情報を前記可搬媒体の前記第1記憶領域に書き込む書込部を備えることを特徴とする器。

【００１６】

また、本発明は、前記利用機器であって、前記可搬媒体は、コンテンツの利用に必要な暗号化されたコンテンツ鍵を記憶する第3記憶領域を備え、前記利用機器は、前記可搬媒体が記憶する第3記憶領域から、当該機器に対応する暗号化コンテンツを読み出す読出部を備えることを特徴とする。

また、本発明は、前記利用機器であって、前記可搬媒体は、コンテンツの利用に必要な暗号化されたコンテンツ鍵を記憶する第3記憶領域と、前記コンテンツ鍵で暗号化されたコンテンツを記憶する第4記憶領域を備え、前記利用機器は、前記可搬媒体が記憶する第4記憶領域から、暗号化されたコンテンツを読み出す読出部を備えることを特徴とする。

【００１７】

また、本発明は、前記利用機器であって、前記可搬媒体は、コンテンツの利用に必要な暗号化されたコンテンツ鍵を記憶する第3記憶領域を備え、前記利用機器は、前記可搬媒体が記憶する第3記憶領域から、当該機器が求める暗号化コンテンツ鍵が存在するか否かを判断する判断部を備えることを特徴とする。

また、本発明は、データを記録する可搬媒体であって、前記可搬媒体は、コンテンツを利用する利用機器を識別可能な機器識別情報を記憶する第1記憶領域、及び当該可搬媒体を識別可能な媒体識別情報を記憶する第2記憶領域を備えることを特徴とする。

【００１８】

また、本発明は、前記可搬媒体であって、前記可搬媒体は、コンテンツの利用に必要な

暗号化されたコンテンツ鍵を記憶する第3記憶領域を備えることを特徴とする。
また、本発明は、前記可搬媒体であって、前記可搬媒体は、メモリーカードであることを特徴とする。
また、本発明は、前記可搬媒体であって、前記可搬媒体は、ICカードであることを特徴とする。
【００１９】
また、本発明は、不正利用を管理する管理機器と、データを記録する可搬媒体からなる不正利用検知システムであって、前記可搬媒体は、利用機器を識別可能な機器識別情報を記憶する第1記憶領域、及び当該可搬媒体を識別可能な媒体識別情報を記憶する第2記憶領域を備え、前記管理機器は、前記可搬媒体の第1記憶領域、及び第2記憶領域からそれぞれ機器識別情報、及び媒体識別情報を読み出す読出部と、前記読み出した機器識別情報、及び媒体識別情報から、前記機器識別情報を保有する利用機器が不正利用されたか否かを判断する判断部を備えることを特徴とする。
【００２０】
また、本発明は、前記不正利用検知システムであって、前記管理機器は、前記機器識別情報と前記媒体識別情報の組を管理する管理テーブルを生成するテーブル生成部と、前記媒体識別情報を基準にして、異なる機器識別情報を入手した場合に当該利用を不正と判断する判断部を備えることを特徴とする。
また、本発明は、前記不正利用検知システムであって、前記管理機器は、前記媒体固有情報ごとに異なるしきい値を設けて記憶する記憶部を備えることを特徴とする。
【００２１】
また、本発明は、不正利用を管理する管理機器であって、データを記録する可搬媒体は、利用機器を識別可能な機器識別情報を記憶する第1記憶領域、及び当該可搬媒体を識別可能な媒体識別情報を記憶する第2記憶領域を備え、前記管理機器は、前記可搬媒体の第1記憶領域、及び第2記憶領域からそれぞれ機器識別情報、及び媒体識別情報を読み出す読出部と、前記読み出した機器識別情報、及び媒体識別情報から、前記機器識別情報を保有する利用機器が不正利用されたか否かを判断する判断部を備えることを特徴とする。
【００２２】
また、本発明は、前記管理機器であって、前記管理機器は、前記機器識別情報と前記媒体識別情報の組を管理する管理テーブルを生成するテーブル生成部と、前記媒体識別情報を基準にして、異なる機器識別情報を入手した場合に当該利用を不正と判断する判断部を備えることを特徴とする。
また、本発明は、前記管理機器であって、前記管理機器は、前記媒体固有情報ごとに異なるしきい値を設けて記憶する記憶部を備えることを特徴とする。
【００２３】
また、本発明は、コンテンツを利用する利用機器と、利用機器の不正を管理する管理機器と、データを記録する可搬媒体からなる不正機器検知方法であって、前記利用機器は、当該機器を識別可能な機器識別情報を記憶する記憶ステップを備え、前記可搬媒体は、前記機器識別情報を記憶する第1記憶ステップ、及び当該可搬媒体を識別可能な媒体識別情報を記憶する第2記憶ステップを備え、前記管理機器は、前記可搬媒体の第1記憶領域、及び第2記憶領域からそれぞれ機器識別情報、及び媒体識別情報を読み出す読出ステップと、前記読み出した機器識別情報、及び媒体識別情報から、前記機器識別情報を保有する利用機器が不正機器か否かを判断する判断ステップを備えることを特徴とする。
【発明の効果】
【００２４】
本発明によれば、効率的に無効化すべき鍵を発見、あるいは特定することが可能である。
【発明を実施するための最良の形態】
【００２５】
以下、本発明の実施の形態について、図面を参照しながら説明する。図1は、本発明に

係る不正機器検知システムの全体構成を示すブロック図である。このシステムは、コンテンツを利用するために必要なコンテンツ鍵の要求が正規機器からであるか不正機器からであるかを判断する管理機器101と、管理機器101に対して、コンテンツ利用者（以下、利用者）の要望に応じてコンテンツ鍵を要求する店舗機器102と、利用者が利用するコンテンツ鍵を格納するための可搬媒体103と、同じく利用者が保有してコンテンツの再生を行う再生機器104からなる。

【００２６】

まず利用者は、可搬媒体103を自身が保持する再生機器104に挿入して、再生機器104から当該端末を一意に特定するための情報（機器ID）を取得して記録する。

次に利用者は、可搬媒体103と店舗機器102を利用して、例えば、視聴したいコンテンツのタイトルを入力するなどして、必要なコンテンツ鍵を要求すると共に、可搬媒体103を店舗機器102に挿入する。利用者からの要求を受け付けた店舗機器102は、コンテンツ鍵を管理機器101に要求すると共に、可搬媒体が保持する自身を一意に特定する情報（媒体ID）と、再生機器104から取得して記録した機器IDを管理機器101に送信する。

【００２７】

最後に、店舗機器102からのコンテンツ鍵要求、媒体ID、並びに機器IDを受信した管理機器101は、前記要求が正規機器からの要求か、不正機器からの要求かを判断して、正規機器からの要求であると判断した場合に、前記要求に対応したコンテンツ鍵を暗号化して、店舗機器102へ送信する。店舗機器102は、受信した暗号化コンテンツ鍵を利用者の可搬媒体103に記録して、利用者は暗号化コンテンツ鍵が記録された可搬媒体103を再生機器104に挿入してコンテンツの視聴を行う。

【００２８】

このとき、視聴するコンテンツ自身は、再生機器104がディスク経由で入手しても、ネットワークを介して入手し蓄積している形態でも、何れの構成であってもよい。以降では、再生機器104は、ネットワーク経由でコンテンツを取得して、内部に蓄積している構成で説明を行う。

図2は、本発明の実施の形態における、管理機器101の機能を示す機能ブロック図である。

【００２９】

管理機器101は、店舗機器102から、コンテンツ鍵の要求、媒体ID、並びに機器IDを受信し、かつ暗号化コンテンツ鍵を送信する送受信部201と、送受信部201で受信した媒体ID、並びに機器IDから、正規機器からの要求であるか否かを判断する判断部202と、判断部202で正規機器からの要求か否かを判断する際に利用する管理テーブルを記憶する管理テーブル記憶部203と、コンテンツを復号するために必要なコンテンツ鍵を記憶するコンテンツ鍵記憶部204と、受信した要求に応じて適当なコンテンツ鍵を選択する選択部205と、機器IDに対応するデバイス鍵を記憶するデバイス鍵テーブル記憶部206と、選択したコンテンツ鍵を受信した機器IDに対応するデバイス鍵で暗号化する暗号化部207を備える。

【００３０】

次に、管理機器101が記憶する管理テーブル300、並びにデバイス鍵テーブル400のデータ形式の一例を図3、並びに図4を用いて説明する。

図3は、管理テーブル300の一例を示している。管理テーブル300は、機器IDを記憶する機器ID記憶領域301と、媒体IDを記憶する媒体ID記憶領域302と、1つの機器IDに対する媒体IDの延べ数を記憶する媒体ID数記憶領域303から構成される。管理テーブル300では、機器IDを基準として、受信した媒体IDを機器IDと対応付けて記録している。図3の例では、機器ID：ID—Aに対しては、2種類の媒体ID：MID—1、MID—5が対応付けて記憶されており、これは、あるタイミングで、ID—AとMID—1の組を管理機器101が受信して、異なるタイミングで、ID—AとMID—5の組を管理機器101が受信したことを意味している。また、この場合、機器ID：ID—Aに対応付けて記憶される媒体IDは2種類となるため、媒体ID数記憶領域303は「2」を示す。

【００３１】

図4は、デバイス鍵テーブル400の一例を示している。デバイス鍵テーブル400は、機器IDを記憶する機器ID記憶領域401と、機器IDに対応するデバイス鍵を記憶するデバイス鍵記憶領域402から構成される。図4の例では、機器ID：ID—Aに対応するデバイス鍵はDK—A、機器ID：ID—Bに対応する鍵はDK—Bとしている。ここで、デバイス鍵の個数は1つである必要はなく複数であってもよく、さらにデバイス鍵が複数の機器IDで共有されている構成であってもよい。

【００３２】

次に、図5を用いて管理機器101の動作について説明する。

S501：店舗機器102から、コンテンツ鍵要求、媒体ID、並びに機器IDを受信する。

S502：管理テーブル300を参照して、S501で受信した機器IDが既に登録されているか否かを判断する。

S503：登録されている場合は、S505の処理へ進み、登録されていない場合は、S504の処理へ進む。

【００３３】

S504：S501で受信した機器IDを管理テーブル300に登録してS507の処理へ進む。

S505：S501で受信した媒体IDが、同じく受信した機器IDに対応付けて管理テーブル300に登録されているか否かを判断する。

S506：登録されている場合は、S508の処理へ進み、登録されていない場合は、S507の処理へ進む。

【００３４】

S507：S501で受信した媒体IDを、同じく受信した機器IDに対応付けて管理テーブル300に登録する。

S508：管理テーブル300の媒体ID数記憶領域を参照して、前記領域の示す値が、予め定められたしきい値を越えているか否かを判断する。

S509：越えていない場合は、S510の処理へ進み、越えている場合は、S511の処理へ進む。

【００３５】

S510：S501で受信した機器IDを基にデバイス鍵テーブル400を参照して対応するデバイス鍵を取得して、さらに要求されたコンテンツ鍵を選択して、取得したデバイス鍵で選択したコンテンツ鍵を暗号化して、暗号化コンテンツ鍵を店舗機器102に対して出力し、処理を完了する。

S511：不正機器からの要求と判断して処理を止める。

【００３６】

図6は、本発明の実施の形態における、可搬媒体103の記憶領域を示す図である。

可搬媒体103は、媒体IDを記憶する書き換えできない領域である媒体ID記憶領域601と、再生機器104から取得した機器IDを記憶する機器ID記憶領域602と、機器IDに対応して取得した暗号化コンテンツ鍵を記憶する暗号化コンテンツ鍵記憶領域603から構成される。図6の例では、可搬媒体103の機器ID記憶領域602には、2種類の機器ID：ID—A、ID—Bが記憶され、暗号化コンテンツ鍵記憶領域603には、ID—Aに対応する暗号化コンテンツ鍵：Enc(DK—A，CK)が記憶されている。ただし、関数Enc(X，Y)は、データYを、鍵データXを用いて暗号化する関数として用いる。従って、Enc(DK—A，CK)は、コンテンツ鍵：CKが、機器ID：ID—Aに対応するデバイス鍵：DK—Aで暗号化された暗号化コンテンツ鍵であることを意味する。

【００３７】

図7は、本発明の実施の形態における、再生機器104の機能を示す機能ブロック図である。

再生機器104は、当該機器を一意に識別する情報（機器ID）を記憶する機器ID記憶部701と、挿入された可搬媒体103から暗号化コンテンツ鍵を読み出す、かつ機器IDを書き込む入出力部702と、デバイス鍵を記憶するデバイス鍵記憶部703と、読み出した暗号化コンテンツ鍵をデバイス鍵で復号する復号部704と、ネットワークを介して受信したコンテンツ

を記憶する暗号化コンテンツ記憶部705と、暗号化コンテンツを、復号して得たコンテンツ鍵で復号する復号部705を備える。

【００３８】

次に、図8を用いて再生機器104の動作について説明する。

S801：可搬媒体103が挿入されると、可搬媒体103の機器ID記憶領域603から機器IDを読み出して、自身の機器IDが登録されているか否かを判断する。

S802：登録されている場合は、S803の処理へ進み、登録されていない場合は、S804の処理へ進む。

【００３９】

S803：自身の機器IDを機器ID記憶領域603に登録して処理を完了する。

S804：可搬媒体103の暗号化コンテンツ鍵記憶領域602を読み出して、自身の機器IDに対応する暗号化コンテンツ鍵が存在するか否かを判断する。

S805：存在する場合は、S806の処理へ進み、存在しないな場合は処理を完了する。

S806：自身の機器IDに対応する暗号化コンテンツ鍵を読み出して、自身が保有するデバイス鍵で復号してコンテンツ鍵を得る。

【００４０】

S807：さらに、コンテンツ記憶部705に記憶する暗号化コンテンツを読み出して、S806で得たコンテンツ鍵で復号してコンテンツを得る。

通常、不正機器の台数は1,000台、もしくは10,000台のオーダであると考えられ、逆に、個人が所有する可搬媒体の上限は100枚あれば十分である。従って、例えばしきい値を100とした場合、可搬媒体を複数所有するユーザであっても、機器IDを基準に媒体IDをカウントすると、その数が100を越えることはない。また、流通する同じ機器IDを持つ不正機器は、それぞれの利用者が保持する可搬媒体の媒体IDが異なるため、不正機器が1,000台存在する場合は、機器IDを基準に媒体IDをカウントするとその数は1,000を越えるため、しきい値である100を越えた時点で、当該機器IDは不正機器で利用されていると判断することが可能となる。

【００４１】

（その他の変形例）

（１）本発明の実施の形態では、再生機器が保有するコンテンツは、ネットワークを介して入手する構成としたが、本発明はその構成に限定されるものではない。例えば、コンテンツを記録する光ディスク等の大容量メディアが再生機器に挿入され、挿入されたメディアからコンテンツを読み出して再生する構成であってもよい。また、可搬媒体に暗号化コンテンツ鍵と共に暗号化コンテンツも記録されており、コンテンツを可搬媒体から入手する構成であってもよい。

【００４２】

（２）本発明の実施の形態では、コンテンツはコンテンツ鍵で暗号化されており、コンテンツ鍵はデバイス鍵で暗号化されている鍵階層としたが、本発明はその構成に限定されるものではない。例えば、鍵階層を追加して、コンテンツはコンテンツ鍵で暗号化され、コンテンツ鍵はメディア鍵で暗号化され、メディア鍵がデバイス鍵で暗号化されるような鍵階層であってもよく、鍵階層に特段の制限は必要ない。

【００４３】

（３）本発明の実施の形態では、コンテンツを利用する正規機器、あるいは不正機器を判断して、不正機器を検知するシステム構成としたが、本発明はその構成に限定されるものではない。例えば、本発明をコンテンツ利用システムに適用する代わりに、電車などの定期券利用システムに応用して、その利用が正規利用か、不正利用かを管理機器が判断して、不正利用を検知する応用システムとしてもよい。例えば、機器IDを持つ携帯端末と、定期券情報が記録され、媒体IDを持つ可搬媒体のペアで動作する定期券システムを仮定する。管理機器は、機器IDと媒体IDの組を管理しており、例えば、ある可搬媒体が他人の携帯端末に挿入されて利用された場合に、管理機器は、当該媒体IDが、異なる機器IDとの組で利用されたことを判断できるため、可搬媒体の不正利用を検知することが可能となる。

さらに、この場合でも、しきい値を設けておき、1つの可搬媒体が利用できる機器の数（機器IDの数）を設定可能な構成であってもよい。その他、機器IDと媒体IDを利用して不正機器、あるいは不正利用を検知するシステムであれば、前記以外のシステムにおいても本発明は適用可能である。

【００４４】

（４）本発明の実施の形態では、利用者は可搬媒体を保持して店舗機器を利用する形態としたが、本発明はその構成に限定されるものではない。例えば、MACアドレスを媒体IDの代わりに使用して、ネットワークを介して、機器ID、並びにMACアドレスを管理機器に送信して、暗号化コンテンツ鍵を受け取る構成であってもよい。その他、MACアドレス以外でも、書き換えできない固有情報を持つ、例えばICカードを利用する形態であってもよく、本発明は書き換え、あるいは変更できない固有情報を利用する形態であれば、如何なる構成であってもよい。

【００４５】

（５）本発明の実施の形態では、可搬媒体は固有な媒体IDを保持する形態としたが、本発明はその構成に限定されるものではない。例えば、定められた（管理可能な）複数の可搬媒体が同じ媒体IDを持つ構成であってもよい。

（６）本発明の実施の形態では、不正機器か否かを判断するためのしきい値は1つとしているが、本発明はその構成に限定されるものではない。例えば、しきい値が複数存在して、1つ目のしきい値を越えた場合は不正機器と判断する前に警告を発して、2つ目のしきい値を越えた場合に不正機器と判断するという構成であってもよい。さらに、機器IDごとに1つ以上のしきい値が設定されている構成であってもよい。

【００４６】

（７）本発明の実施の形態では、可搬媒体が記録するデータは、機器ID、暗号化コンテンツ鍵としたが、本発明はその構成に限定されるものではない。例えば、各コンテンツには、それぞれを一意に識別するための識別情報（コンテンツID）が管理用として付与されており、暗号化コンテンツ鍵を記録する際は、当該コンテンツ鍵で復号可能なコンテンツのコンテンツIDも合わせて記録する構成であってもよい。さらに、利用者、あるいは利用機器は、所望のコンテンツを、前記コンテンツIDを用いて選択する構成であってもよい。

【産業上の利用可能性】

【００４７】

本発明にかかる不正機器検知システムは、管理機器に対するコンテンツ鍵の要求が正規機器からの要求か、不正機器からの要求かを判断することで、効率よく不正機器を検知することが可能となり、より効果的な著作権の保護を実現できるという効果を有する。

【図面の簡単な説明】

【００４８】

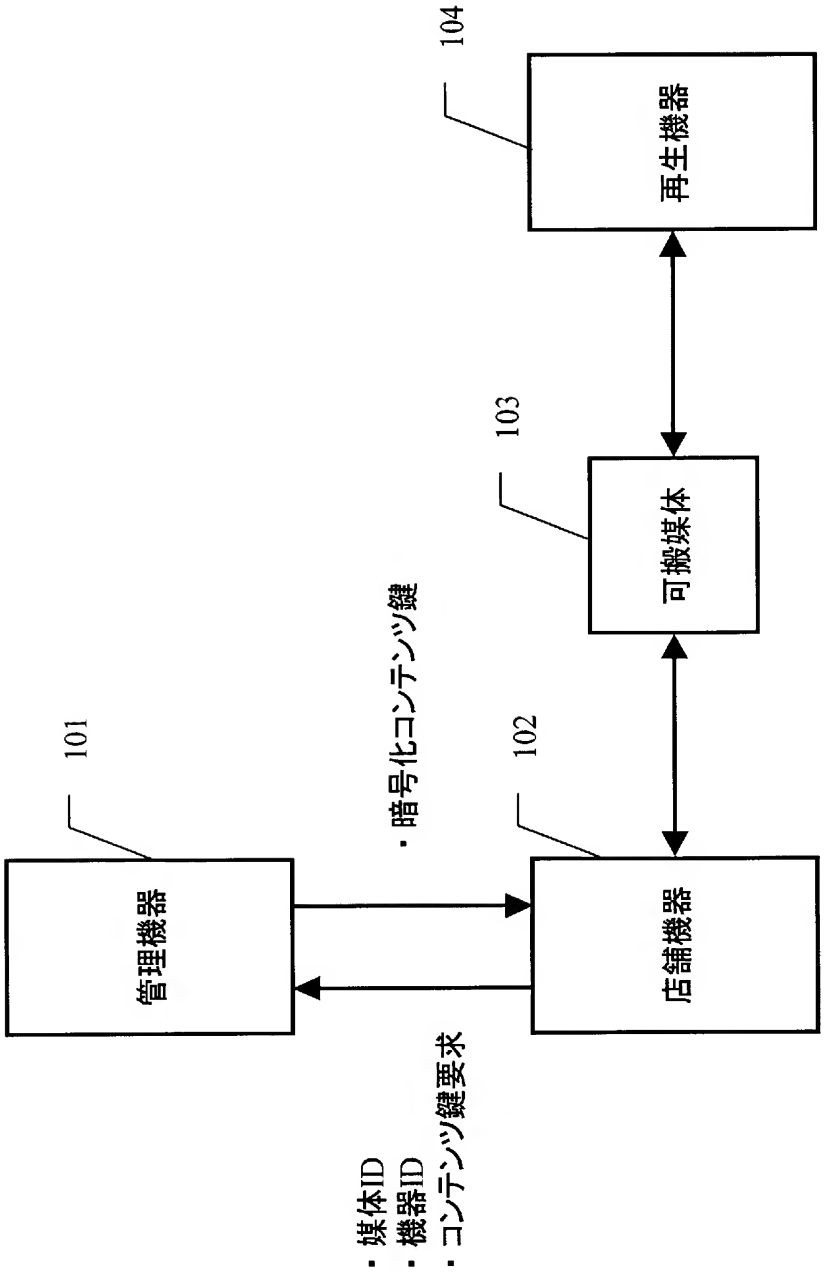
【図１】本発明に係る不正機器検知システムの全体構成を示すブロック図
【図２】本発明の実施の形態における管理機器の機能を示す機能ブロック図
【図３】本発明の実施の形態における管理機器が保持する管理テーブルの例
【図４】本発明の実施の形態における管理機器が保持するデバイス鍵テーブルの例
【図５】本発明の実施の形態における管理機器の動作を示すフロー
【図６】本発明の実施の形態における可搬媒体が保持するデータの例
【図７】本発明の実施の形態における再生機器の機能を示す機能ブロック図
【図８】本発明の実施の形態における再生機器の動作を示すフロー

【符号の説明】

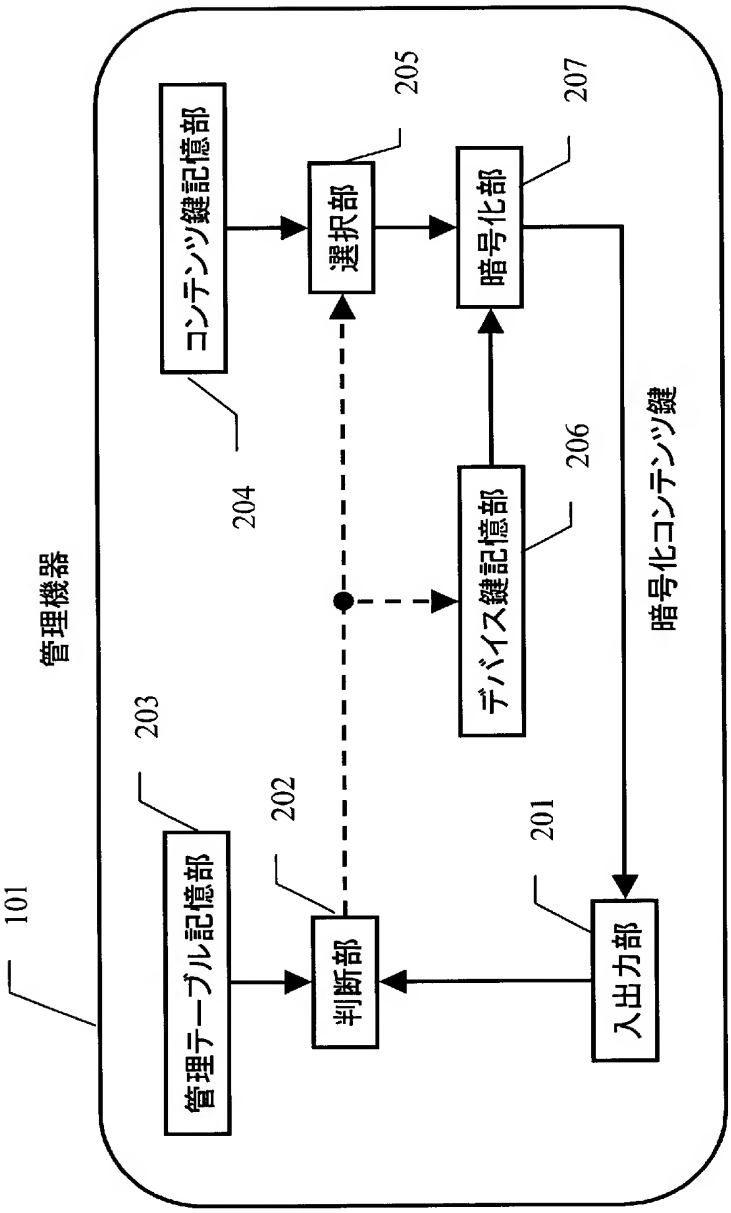
【００４９】

101 管理機器
102 店舗機器
103 可搬媒体
104 再生機器

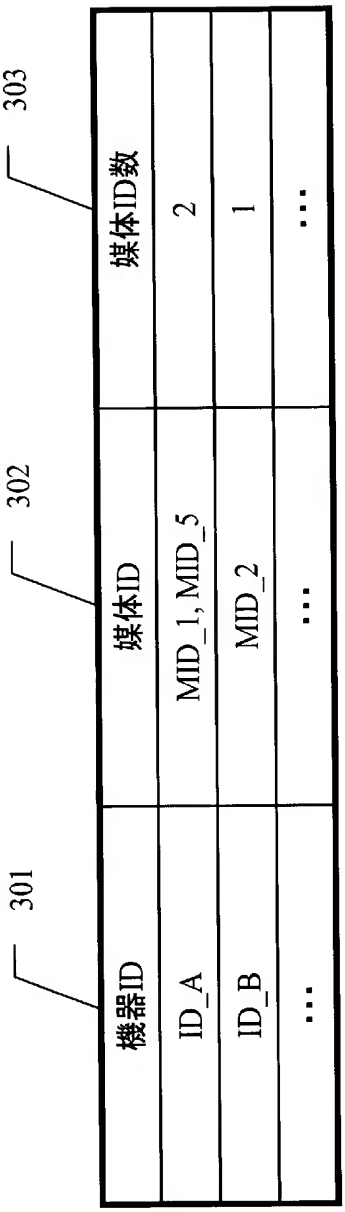
【書類名】図面
【図１】


104
再生機器
103
可搬媒体
101
管理機器
・暗号化コンテンツ鍵
102
店舗機器
・媒体ID
・機器ID
・コンテンツ鍵要求

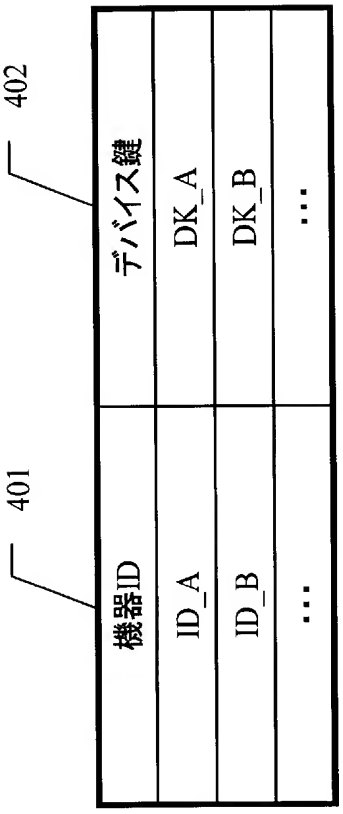
【図２】


101
管理機器
203
管理テーブル記憶部
202
判断部
201
入出力部
204
コンテンツ鍵記憶部
205
選択部
206
デバイス鍵記憶部
207
暗号化部
暗号化コンテンツ鍵

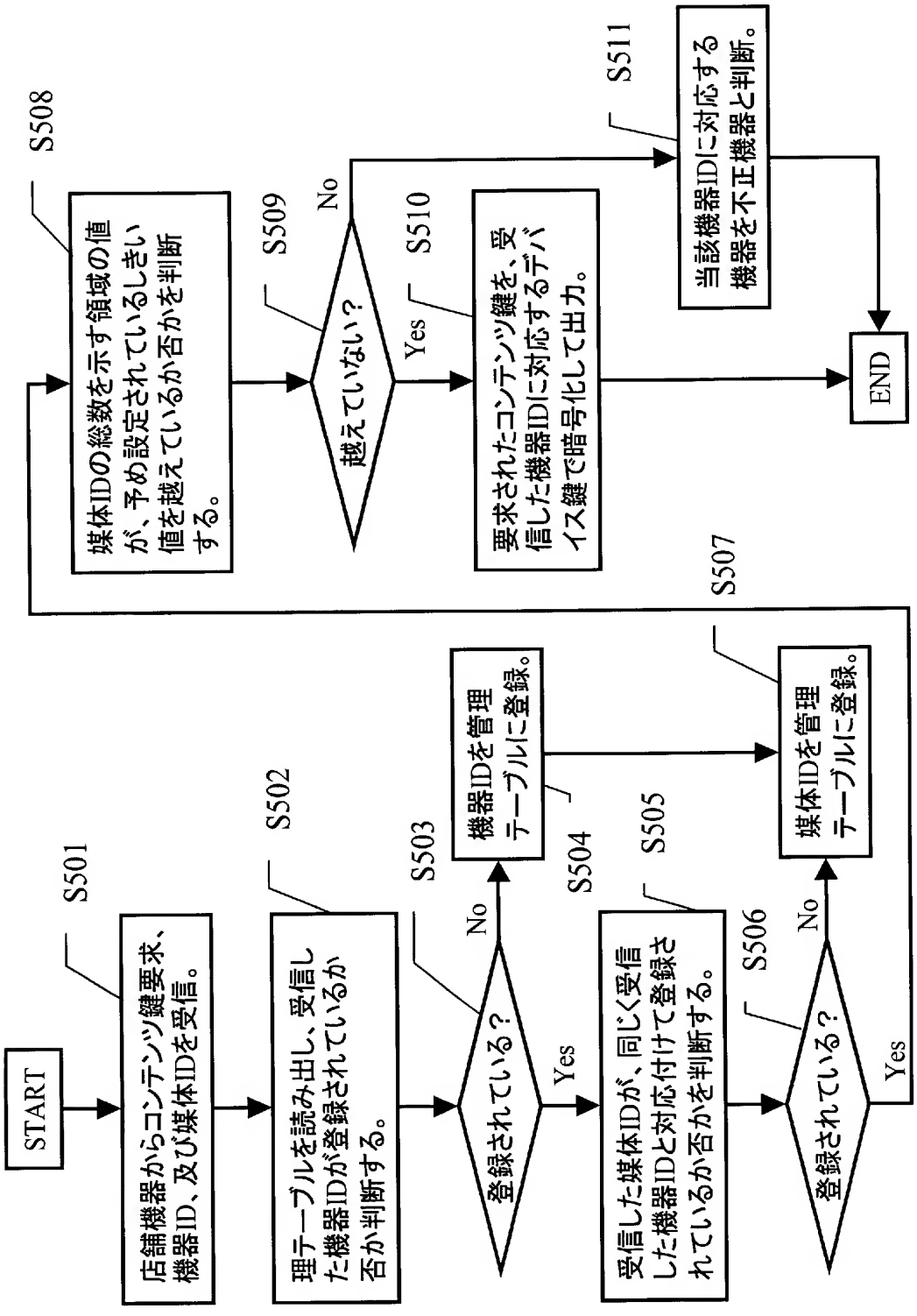
【図３】



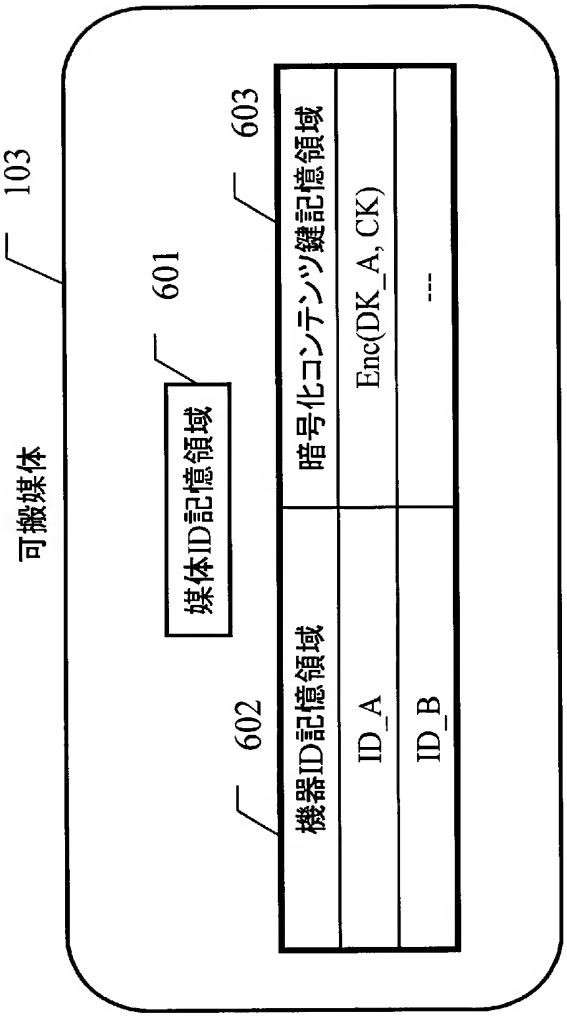
【図４】



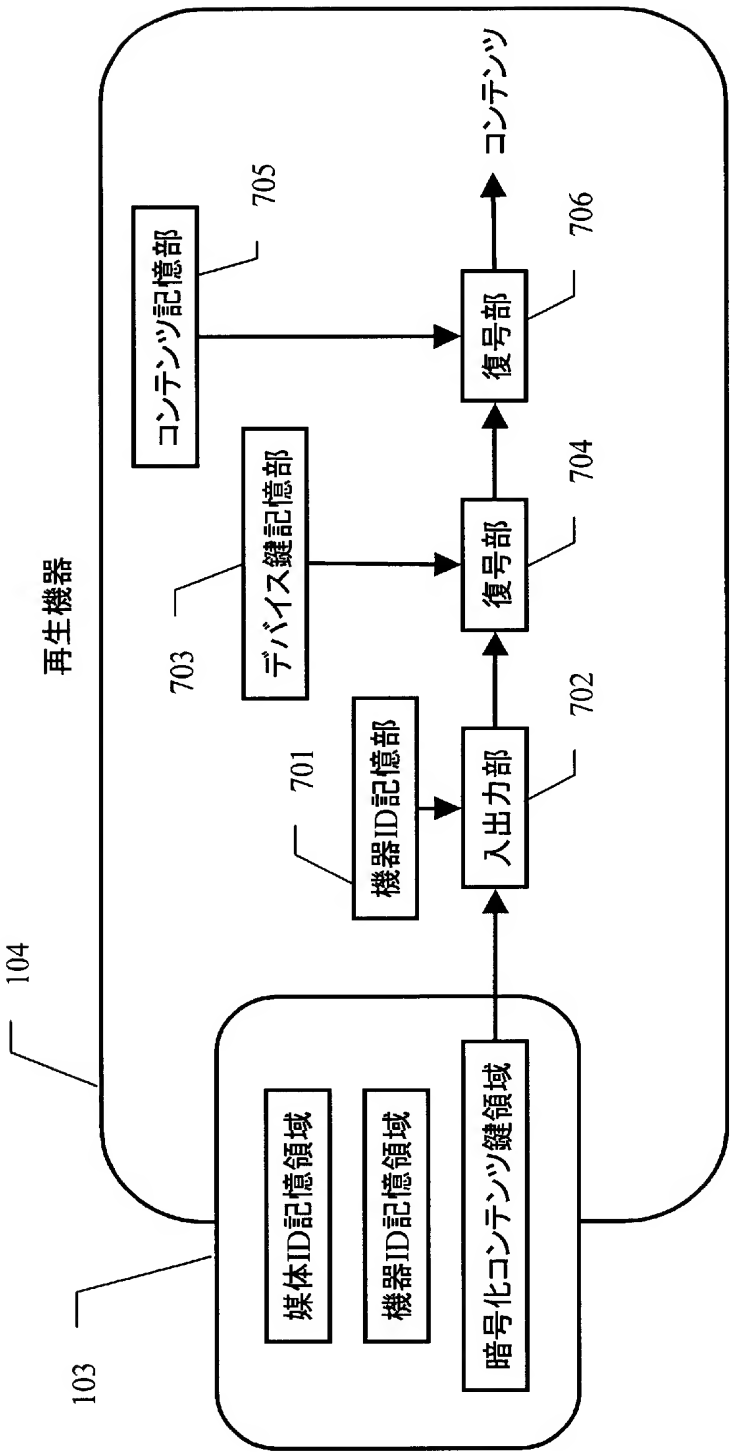
【図５】


START
S501
店舗機器からコンテンツ鍵要求、機器ID、及び媒体IDを受信。
S502
理テーブルを読み出し、受信した機器IDが登録されているか否か判断する。
S503
登録されている？
No
Yes
S504
機器IDを管理テーブルに登録。
S505
受信した媒体IDが、同じく受信した機器IDと対応付けて登録されているか否かを判断する。
S506
登録されている？
No
Yes
S507
媒体IDを管理テーブルに登録。
S508
媒体IDの総数を示す領域の値が、予め設定されているしきい値を越えているか否かを判断する。
S509
越えていない？
No
Yes
S510
要求されたコンテンツ鍵を、受信した機器IDに対応するデバイス鍵で暗号化して出力。
S511
当該機器IDに対応する機器を不正機器と判断。
END

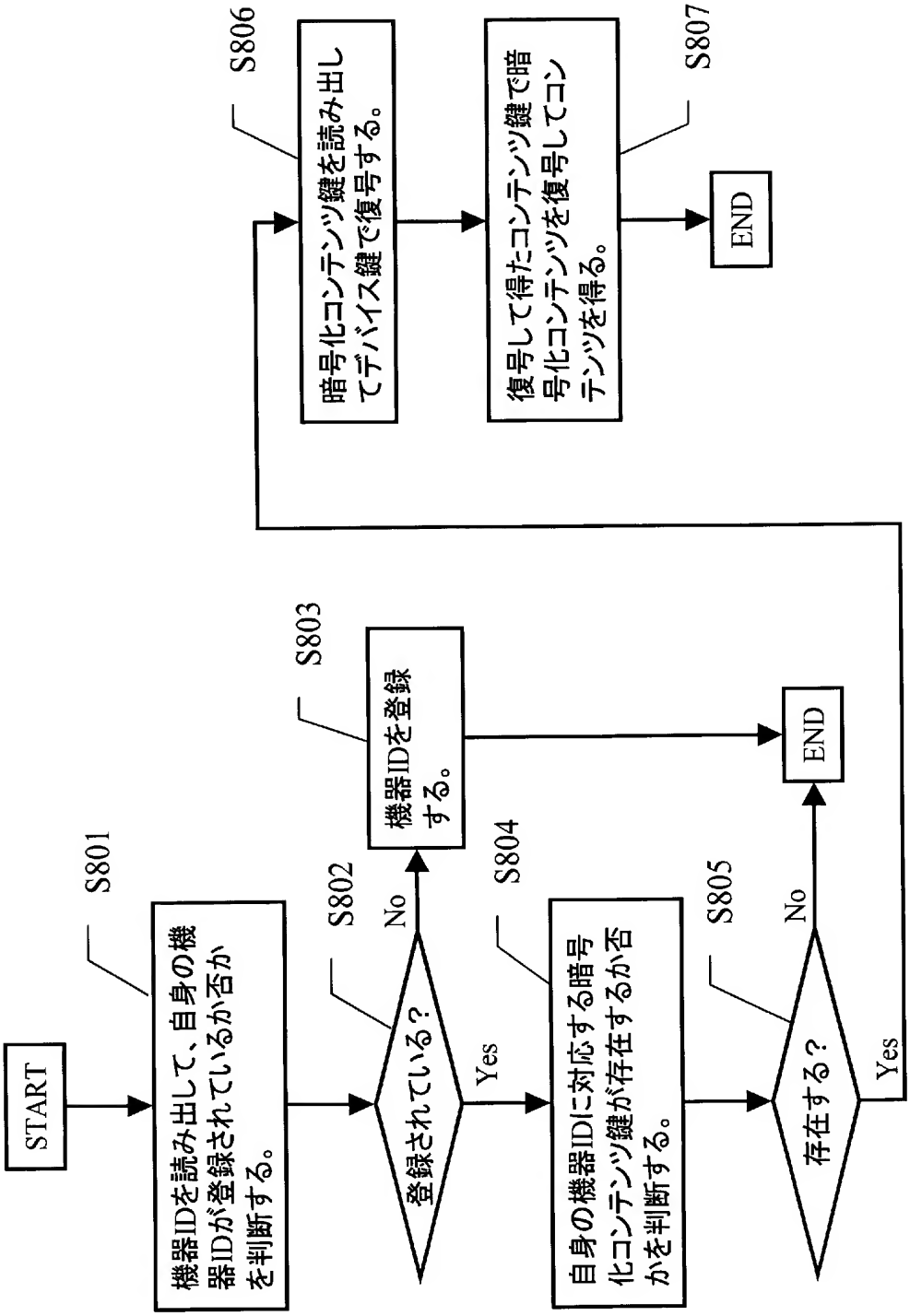
【図６】


103
可搬媒体
601
媒体ID記憶領域
602
603
機器ID記憶領域
暗号化コンテンツ鍵記憶領域
ID_A
Enc(DK_A, CK)
ID_B

【図７】


再生機器
104
103
媒体ID記憶領域
機器ID記憶領域
暗号化コンテンツ鍵領域
入出力部
702
機器ID記憶部
701
復号部
704
デバイス鍵記憶部
703
復号部
706
コンテンツ記憶部
705
コンテンツ

【図８】


START
S801
機器IDを読み出して、自身の機器IDが登録されているか否かを判断する。
S802
登録されている？
No
S803
機器IDを登録する。
END
Yes
S804
自身の機器IDに対応する暗号化コンテンツ鍵が存在するか否かを判断する。
S805
存在する？
No
END
Yes
S806
暗号化コンテンツ鍵を読み出してデバイス鍵で復号する。
復号して得たコンテンツ鍵で暗号化コンテンツを復号してコンテンツを得る。
S807
END

【書類名】要約書
【要約】
【課題】　鍵無効化技術では、外部に漏れた鍵（無効化すべき鍵）を特定する必要があるが、特定するためには、市場に大量流通した不正機器／不正ソフトウェアを回収して、内部を解析することでしか特定できないという課題を有していた。
【解決手段】　正規機器と不正機器を識別するための付加情報（可搬媒体の固有ID）を利用して、管理装置において、正規機器からのアクセスか不正機器からのアクセスかの判定を行い、不正機器の特定を実現する。
【選択図】　図1

【書類名】　手続補正書
【整理番号】　2048160379
【提出日】　平成17年 3月30日
【あて先】　特許庁長官　殿
【事件の表示】
　【出願番号】　特願2004-360437
【補正をする者】
　【識別番号】　000005821
　【住所又は居所】　大阪府門真市大字門真１００６番地
　【氏名又は名称】　松下電器産業株式会社
【補正をする者】
　【識別番号】　504137912
　【住所又は居所】　東京都文京区本郷７－３－１
　【氏名又は名称】　国立大学法人東京大学
【代理人】
　【識別番号】　100090446
　【住所又は居所】　大阪市北区豊崎３丁目２番１号淀川５番館６Ｆ
　【弁理士】
　【氏名又は名称】　中島　司朗
【発送番号】　018263
【手続補正1】
　【補正対象書類名】　特許願
　【補正対象項目名】　提出物件の目録
　【補正方法】　追加
　【補正の内容】
　　【提出物件の目録】
　　【物件名】　持分について証明する書面　1

【物件名】　　持分について証明する書面

東大―松下電器連携契約準拠

【添付書類】

持分証明書

平成１７年１月２８日

事件の表示　　平成１６年１２月１３日付特許願 2004-360437 号
整理番号　　(20481)H16-0379(乙内：依頼番号)
3004Z013-1（甲内：整理番号）

上記発明の特許を受ける権利の持分を国立大学法人 東京大学 50%、松下電器産業株式会社 50%と定めたことに相違ありません。

東京都文京区本郷七丁目三番一号
国立大学法人 東京大学
総長　佐々木　毅

大阪府門真市大字門真１００６番地
松下電器産業株式会社
取締役社長　　中村　邦夫

【書類名】　手続補正書
【整理番号】　2048160379
【提出日】　平成17年 8月 1日
【あて先】　特許庁長官　殿
【事件の表示】
　【出願番号】　特願2004-360437
【補正をする者】
　【識別番号】　000005821
　【住所又は居所】　大阪府門真市大字門真１００６番地
　【氏名又は名称】　松下電器産業株式会社
【補正をする者】
　【識別番号】　504137912
　【住所又は居所】　東京都文京区本郷７－３－１
　【氏名又は名称】　国立大学法人東京大学
【代理人】
　【識別番号】　100090446
　【住所又は居所】　大阪市北区豊崎３丁目２番１号淀川５番館６Ｆ
　【弁理士】
　【氏名又は名称】　中島　司朗
【発送番号】　048476
【手続補正1】
　【補正対象書類名】　手続補正書
　【補正対象書類提出日】　平成17年 3月30日
　【補正対象項目名】　持分について証明する書面
　【補正方法】　変更
　【補正の内容】
　　【提出物件の目録】
　　【物件名】　持分について証明する書面　1

【物件名】　持分について証明する書面

東大—松下電器連携契約準拠

【添付書類】

持分証明書

16 12 13
平成 ~~17~~ 年 ~~8~~ 月 ~~28~~ 日

事件の表示　平成１６年１２月１３日付特許願 2004-360437 号
整理番号　(20481)H16-0379(乙内：依頼番号)
3004Z013-1（甲内：整理番号）

上記発明の特許を受ける権利の持分を国立大学法人 東京大学 50%、松下電器産業株式会社 50%と定めたことに相違ありません。

東京都文京区本郷七丁目三番一号
国立大学法人 東京大学
総長　佐々木　毅

大阪府門真市大字門真１００６番地
松下電器産業株式会社
取締役社長　　中村　邦夫

出願人履歴

０００００５８２１
19900828
新規登録

大阪府門真市大字門真１００６番地
松下電器産業株式会社
５０４１３７９１２
20040406
新規登録

東京都文京区本郷７丁目３番１号
国立大学法人　東京大学